Module : Les réseaux privés virtuels				Code	
				ING-4-SSIR-S8-P1	
Période	**Semestre 8**	*Volume horaire*	**21h**	*ECTS*	**2**

Responsable	**Mr Slim Rkhis**	*email*	Slim.rkhis@gmail.com
Equipe pédagogique	**Mr Slim Rkhis**		

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

L'objectif de ce cours est d'appréhender les concepts, les techniques, et les protocoles, de mise en place de réseaux privés virtuels pour la sécurisation des réseaux d'entreprises. Les différentes solutions de mise en place de VPNs niveaux 2, 3 et 4, à savoir les solutions utilisant les protocoles IPSec, L2TP, PPTP, et SSL/TLS seront examinées en détails, et leurs avantages/faiblesses en sécurité seront discutés.

A l'issue de ce cours, l'étudiant doit être capable de :

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

- Maitriser les aspects d'ingénierie, liés à la mise en place de solutions VPNs (**C1.2**)
- Comprendre les services de sécurité fournis par chaque type de solutions(**C1.1**)
- Savoir choisir, concevoir, et déployer des solutions VPNs. (**C5.2**)

Compétences
C1.3 Tester sur une machine des solutions VPN
C5.2 Les configuration sécurisée des solutions VPN
C1.2 Maitriser le développement des solutions VPN

2. Pré-requis*(autres UE et compétences indispensables pour suivre l'UE concernée)*

Fondements des réseaux, Routage IP, Algorithmes et Protocoles Cryptographique

3. Répartition d'Horaire de Module

Intitulé de l'élément d'enseignement	*Total*	*Cours*	*TD*	*Atelier*	*PR*
Module :…VPN	21	11	4.5	9.5	

4. Méthodes pédagogiques et moyens spécifiques au Module

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)		
- Supports de Cours - Projecteur et Tableau		
Bibliographie		
Titre	**Auteur(s)**	**Edition**
Cryptography And Network Security	William Stallings	2018
Cybersecurity – Attack and Defense Strategies	Yuri Diogenes and Erdal Ozkaya	2019

5. Contenu *(Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique[1])*	Durée allouée	
Séance 1 & 2 : Fondements des VPNs - Besoins de VPNs - Réseaux VPNs de confiance, sécurisés, et hybrides - Encapsulation VPN : Techniques et modes - Fonctions de sécurité des VPNs : Authentification, Contrôle d'accès, intégrité et Confidentialité - VPNs obligatoires et volontaires - Architecture VPN (basée sur les couches du modèle OSI) - Scénarios d'utilisation des VPNs intranet, extranet, et accès à distance	Cours TD TP	3H 3H 0H
Séance 3: Mise en place de VPNs niveau 2 : Utilisation de PPTP et L2TP - Protocole GRE : encapsulation, fonctionnement, et limites - Protocole PPP et techniques et de sécurité - Mise en place de VPNs avec le Protocole PPTP - Tunnels obligatoires et volontaires avec PPTP et scénarios d'utilisation - Mise en place de VPNs avec le Protocole L2TP - Messages, tunnels, et sessions L2TP - Limites de sécurité du protocole L2TP et combinaison avec IPSec	Cours TD TP	0H - 3H
Séance 4 & 5 : Mise en place de VPNs niveau 3 : Utilisation de IPSec	Cours TD	3H 1.5H

1

- Architecture et concepts IPSec - Mode Transport et Mode Tunnel IPSec - Fonctionnement et services du Protocole AH - Fonctionnement et services du Protocole ESP - Configuration des Association de Sécurité IPSec, concepts SA, SAD, et SPD - Utilisation d'Associations de Sécurité multiples - Interopérabilité IPSec et translation d'adresses - IPSec / mobilité IP, évolutivité, et qualité de service - Evolution des backbones et utilization de MPLS - MPLS et IPSec	TP	1.5H
Séance 6: Authentification, contrôle d'accès, et Gestion de clés - Protocole Diffie-Hellman et ses faiblesses - Authentification IKE - VPN et infrastructures de gestion de clés - Protocole IKE : Modes et phases - Protocole IKE : Blocs et types d'échanges - IKE et protection contre les attaques	Cours TP	1.5H 1.5H
Séance 7: SSL/TLS VPNs - Besoin de VPNs niveau Transport - Protocoles SSL et TLS, et principe de fonctionnement - Architecture et sous protocoles SSL et TLS - Solutions VPN SSL/TLS en IPv4 et en IPv6 - Faiblesses et limites des solutions VPN SSL Révision	TP Cours	2H 1h

6. Mode d'évaluation de Module*(nombre, types et pondération des contrôles)*					
Eléments d'enseignement	Coeff	DS	EX	TP	PR
Module - VPN	1	40%	60%		
Pour valider le module, les étudiants passeront un examen dont le coefficient est de 60%, un DS dont le coefficient est de 40% La durée de tous les examens (Examen, DS…) est de 1h30.					

Quant à l'examen, il est planifié après l'écoulement des 7 semaines et portera sur toutes les thématiques enseignées tout au long des 21 heures.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.